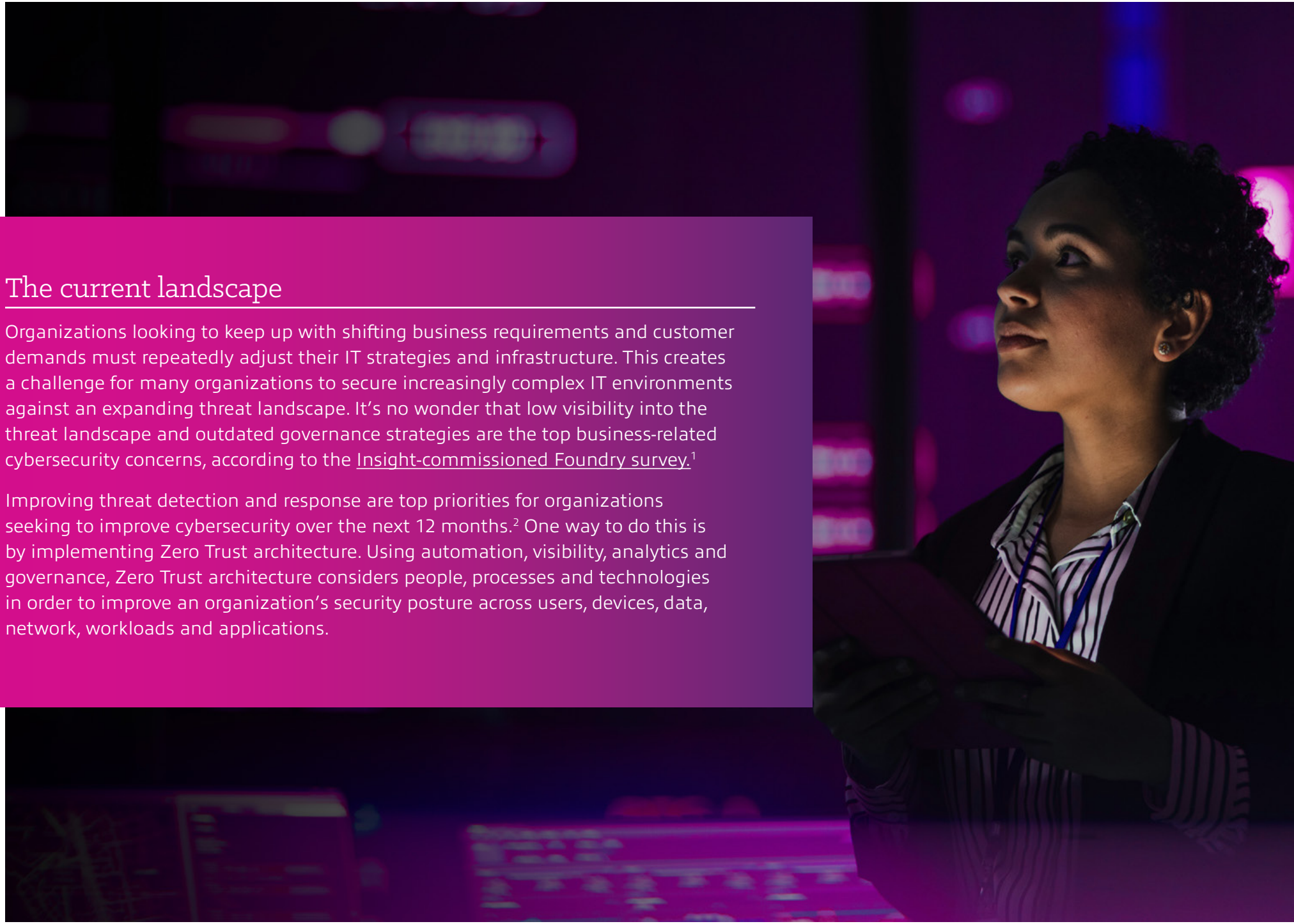
Securing Your Business Assets With Zero Trust Architecture

A guide to designing security solutions using Zero Trust strategies and architectures

Insight®



The current landscape

Organizations looking to keep up with shifting business requirements and customer demands must repeatedly adjust their IT strategies and infrastructure. This creates a challenge for many organizations to secure increasingly complex IT environments against an expanding threat landscape. It's no wonder that low visibility into the threat landscape and outdated governance strategies are the top business-related cybersecurity concerns, according to the Insight-commissioned Foundry survey.[1]

Improving threat detection and response are top priorities for organizations seeking to improve cybersecurity over the next 12 months.[2] One way to do this is by implementing Zero Trust architecture. Using automation, visibility, analytics and governance, Zero Trust architecture considers people, processes and technologies in order to improve an organization's security posture across users, devices, data, network, workloads and applications.

Zero Trust architecture explained

Zero Trust is a security strategy based on the principle "never trust, always verify." Using a Zero Trust architecture, organizations can protect their assets for the long run and strength overall cybersecurity.

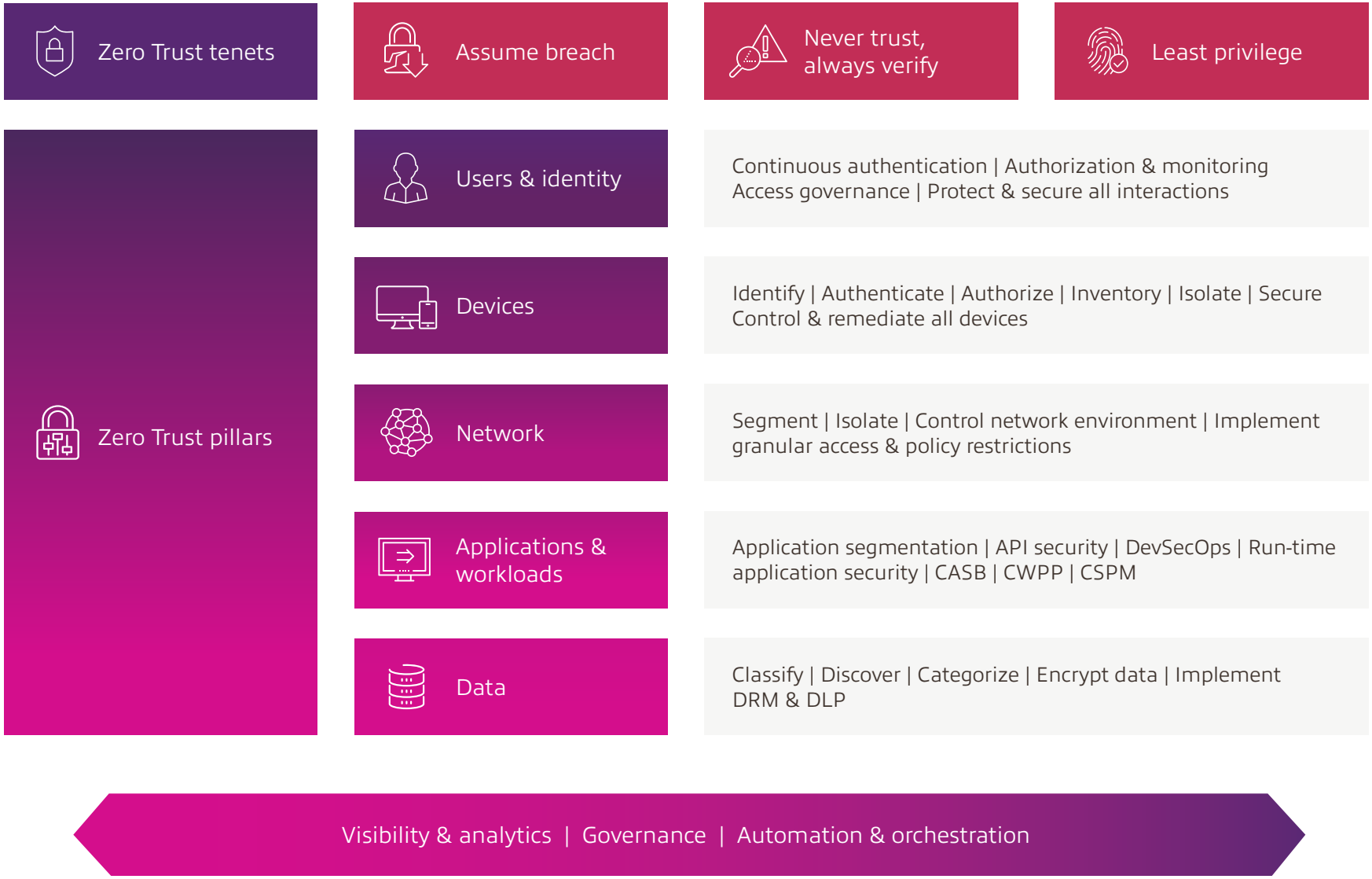
Zero Trust strategy has three key tenets:

- **Assume breach** to develop solutions that minimize the spread of a threat.
- Trust is not implicit: Build solutions that **never trust and always verify** in order to reduce risk.
- **Use least privilege access** so users only have access to what they need to do their jobs.

The three tenets of Zero Trust are applied across five pillars in order to reduce risk and minimize the spread of an attack. The five pillars that make up a Zero Trust architecture are:

These pillars use solutions such as multi-factor authentication, network segmentation and data classification. When an organization implements more mature solutions, such as just-in-time access and analytics, its Zero Trust maturity level improves.

Zero Trust architecture explained (continued)



Each pillar also includes security operations and governance capabilities. These capabilities include visibility and analytics, automation and orchestration, and governance against defined policies and standards. These important features detect anomalous behavior, automate security processes and responses to incidents, and provide threat visibility.

Zero Trust maturity levels

Zero Trust architecture has four maturity levels, according to the Cybersecurity & Infrastructure Security Agency (CISA).[3] The maturity levels can be identified across the five pillars of a Zero Trust architecture depending on the capabilities enabled. As a Zero Trust architecture's solutions across people, processes and technologies become more advanced and automated, its maturity level increases.

Maturity levels

Optimal: The implemented security technologies and processes are using continuous and automated features to manage and detect requests and potential threats across the five pillars. This is the highest level of maturity and something to strive for; however, many organizations may never attain an optimal maturity level as it can take many years.

Advanced: Most processes, controls and configurations are automated to align with policies. Plus, more advanced capabilities are enabled, such as least privilege access and network segmentation. At this level, advanced solutions are enabled consistently across all environments and are being used for threat or out-of-policy visibility and analytics.

Initial: Policies are clearly established and better governed. Although governance may be manual, some processes at this stage are becoming automated. Some enhanced security solutions are enabled, such as multi-factor authentication.

Traditional: This maturity level is where most organizations start. Processes are manual, policies are not strictly enforced and may not be fully designed, and validation is not done continuously. At this maturity level, organizations may be considering advanced security solutions, but these solutions are not enabled.

Key benefits of Zero Trust

Reduce security threat exposure.

Continuous verification of users and devices on your network helps detect and prevent malicious activities in near real time. Using least privilege concepts helps mitigate insider threats such as attackers posing as internal users.

Minimize lateral movement of attacks.

Capabilities such as micro- and macro-segmentation and strong access controls limit the attack surface and help prevent an attacker from accessing and exfiltrating sensitive data.

Improve threat visibility and response.

By continuously analyzing user and network data, anomalous traffic patterns can be easily detected. Additional controls, such as secondary authentication prompts, assist with prevention of threat actor activities.

Zero Trust success factors: People, processes and technologies

Zero Trust is about more than just technology and products. Of course, security technologies play a large role in sophisticated and efficient management of endpoints and users by monitoring and managing devices, users and vulnerabilities within your environment. However, without trained users and defined processes, these technologies are not as effective. That's why when designing your cybersecurity strategy using a Zero Trust architecture, you must consider people, processes and technologies.

Not only do you need IT experts who can respond to incidents and remediate vulnerabilities, but you also need to train your end users about the importance of keeping their credentials and sensitive data secure. To do this, you must establish processes defining what is acceptable or unacceptable. Established processes for people and technology will maximize the reduction of risk and minimize lateral movement of attacks. Together, processes, people and technologies enable governance, visibility and automation, fortifying your organization's overall security posture.

Learn more about Zero Trust.

Explore these resources for more context on what it means to successfully implement a Zero Trust architecture.

Mitigating Risk & Avoiding Technical Debt Through a Zero Trust Framework

Watch this webcast to learn how a Zero Trust approach to cybersecurity can help your organization reduce risk and optimize your overall IT strategy.

Securing the Modern Workplace With SASE for Zero Trust

Discover how Secure Access Service Edge (SASE) solutions prioritize visibility, shared data and consistent policies to support a Zero Trust framework for ground-up protection against evolving modern workplace threats.

Actions to get you started on your Zero Trust journey

Organizations today are adopting versions of Zero Trust suited to specific access and control requirements in order to strengthen security postures and protect users and data. Organizations looking to implement Zero Trust should begin with these three steps:

1. Identify your assets.

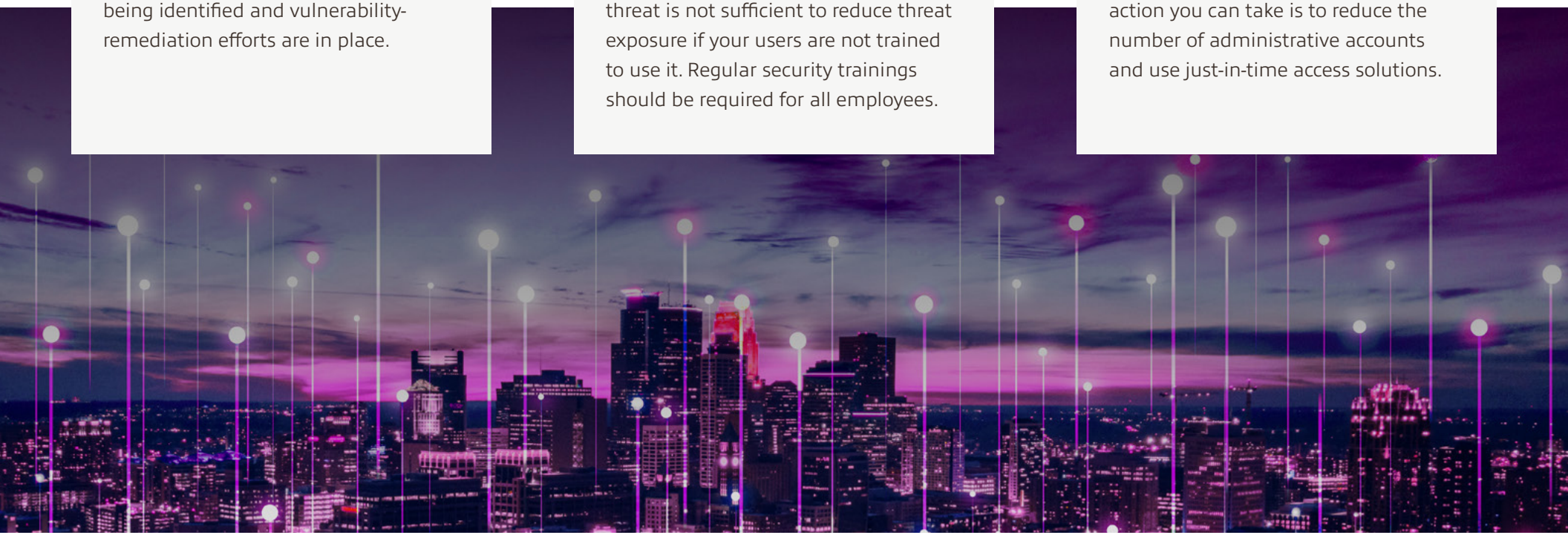
Given the increasing complexity of IT environments, it is important to inventory all your organization's assets, especially business-critical assets and those with access to confidential data. Ensure vulnerabilities are actively being identified and vulnerability-remediation efforts are in place.

2. Mandate user training.

In the past year, 51% of organizations experienced a cybersecurity breach.[4] This reiterates not only the importance of having a trained security team but also the importance of training end users. Obtaining a tool to prevent a threat is not sufficient to reduce threat exposure if your users are not trained to use it. Regular security trainings should be required for all employees.

3. Improve access management.

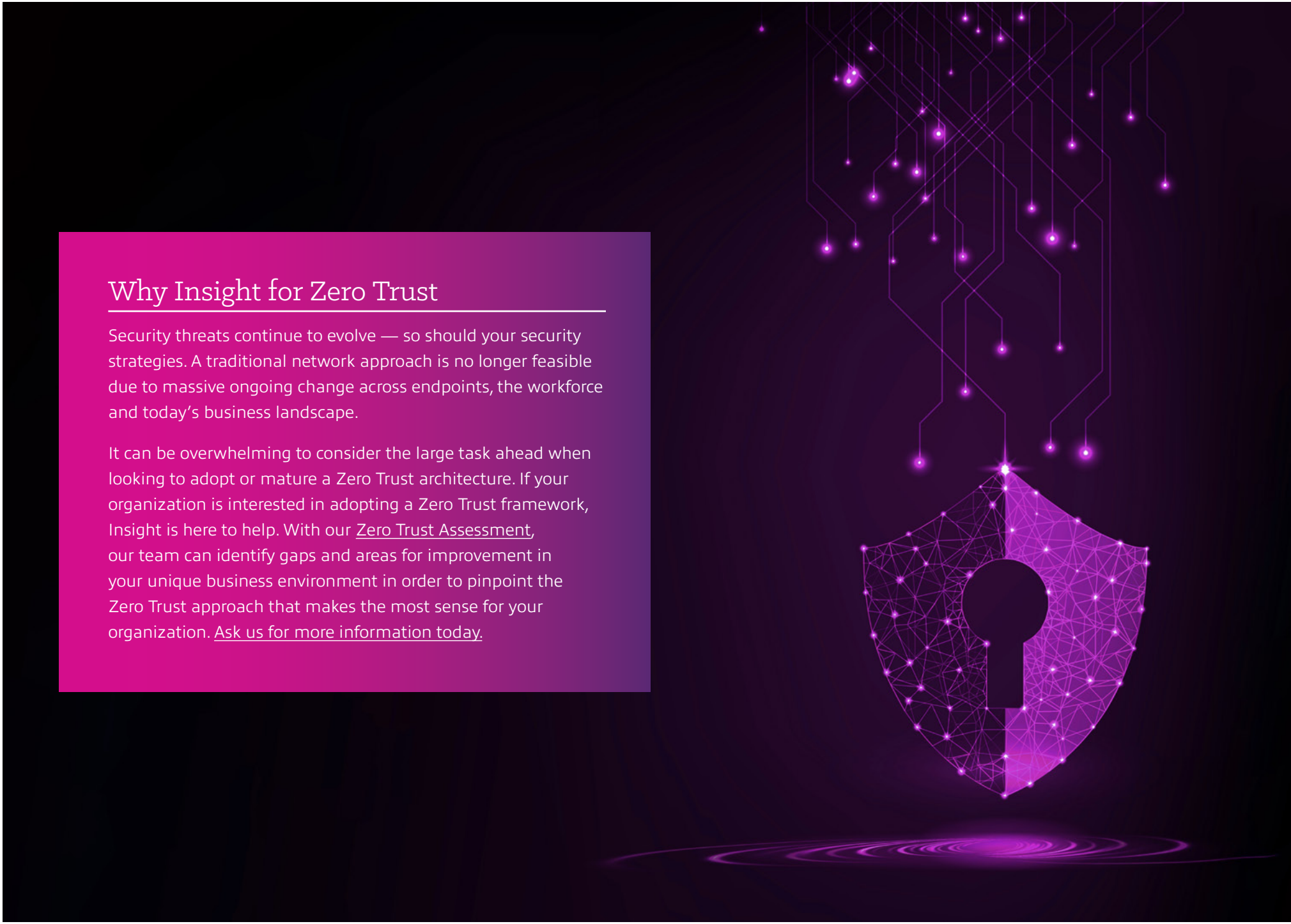
Passwords alone are not enough to protect organizations from data breaches. You can enhance your identity management solution with multi-factor authentication or password-less technologies. Another action you can take is to reduce the number of administrative accounts and use just-in-time access solutions.



Why Insight for Zero Trust

Security threats continue to evolve — so should your security strategies. A traditional network approach is no longer feasible due to massive ongoing change across endpoints, the workforce and today's business landscape.

It can be overwhelming to consider the large task ahead when looking to adopt or mature a Zero Trust architecture. If your organization is interested in adopting a Zero Trust framework, Insight is here to help. With our Zero Trust Assessment, our team can identify gaps and areas for improvement in your unique business environment in order to pinpoint the Zero Trust approach that makes the most sense for your organization. Ask us for more information today.



About Insight

Insight Enterprises, Inc., is a Fortune 500 Solutions Integrator with 13,000 teammates worldwide helping organizations accelerate their digital journey to modernize their business and maximize the value of technology. We enable secure, end-to-end transformation and meet the needs of our clients through a comprehensive portfolio of solutions, far-reaching partnerships and 35 years of broad IT expertise. Rated as a Forbes World's Best Employer and certified as a Great Place to Work, we amplify our solutions and services with global scale, local expertise and a world-class e-commerce experience, realizing the digital ambitions of our clients at every opportunity.

Discover more at insight.com.

Insight®

Sources:

[1]MarketPulse Research by Foundry Research Services. (February 2023). The Path to Digital Transformation: Where Leaders Stand in 2023. Slide 11. Commissioned by Insight.

[2]MarketPulse Research by Foundry Research Services. (February 2023). The Path to Digital Transformation: Where Leaders Stand in 2023. Slide 11. Commissioned by Insight.

[3]Cybersecurity & Infrastructure Security Agency. (April 2023). Zero Trust Maturity Model (Version 2.0).

[4]MarketPulse Research by Foundry Research Services. (February 2023). The Path to Digital Transformation: Where Leaders Stand in 2023. Slide 35. Commissioned by Insight.